Шевердін Д.О., Гаряєва Г.М.
м. Харків, Україна

ПОРІВНЯЛЬНО-ПРАВОВИЙ АНАЛІЗ ЗАКОНОДАВСТВА УКРАЇНИ ТА ЗАРУБІЖНИХ КРАЇН, ЩО РЕГЛАМЕНТУЄ ВІДПОВІДАЛЬНІСТЬ ЗА КОМП'ЮТЕРНІ ЗЛОЧИНИ

Вступ. Інформаційний розвиток суспільства та запровадження на державному рівні в Україні використання мережі Internet та інших комп'ютерних систем в усіх сферах суспільного життя, поряд із позитивними здобутками, супроводжується і негативними явищами. Особливу занепоко-єність викликає збільшення кількості злочинів у сфері використання електрон-но-обчислювальних машин (комп'ютерів), комп'ютерних систем та мереж, як в світі, так і в Україні, оскільки такі злочини не лише гальмують позитивні тенденції розвитку, а й завдають шкоди суспільству, державі, суб'єктам інформаційних відносин в усіх сферах господарювання та окремим громадянам.

Тому мета роботи полягала в дослідженні правопорушень шкідливого програмного забезпечення, яке може мати будь-який користувач, а також робота нолягала у комплексному аналізі об'єктивних і суб'єктивних ознак складу злочину не тільки в Україні, а й в інших зарубіжних країнах. Актуальність боротьби з вказаними злочинами, неоднозначність підходів та висновків наукових досліджень, щодо змісту ознак складу злочину та необхідність створення відповідної світовим вимогам належної вітчизняної правової бази в цій області, обумовили вибір теми цієї статті.

Дослідження та аналіз комп'ютерних злочинів. Сучасні високі технології є одними з основних засобів розвитку всіх сфер суспільного життя та взаємозв'язків міжнародної спільноти. При посередництві комп'ютерних мереж здійснюються функції приватного та публічного характеру, реалізуються завдання держав, фізичних та юридичних осіб у різних сферах життєдіяльності, в тому числі електронна комерція.

Нерозривно з розвитком високих технологій щоденно збільшується кількість протиправних носягань на комп'ютерні системи та комп'ютерну інформацію, що в них зберігається. Такі посягання становлять значну загрозу не лише державним, колективним інтересам, а й інтересам окремих осіб.

Особлива суспільна небезпечність таких злочинів обумовлюється факторами:

1. Інтенсивне впровадження різноманітних інформаційних технологій і процесів, заснованих на використанні електронно-обчислювальних машин, у багатьох сферах людської діяльності;

2. Високий масштабний коефіцієнт зусиль злочинців у цій сфері;

3. Відносна доступність для широкого кола осіб спеціальних знань і техніки, необхідної для вчинення злочину.

Як повідомляється в останній доповіді міжнародного об'єднання у захисті телекомунікаційних технологій Computer Security Institute (CSI), в минулому році більш 85% підприємств і установ Computer Security Institute зіткнулися з випадками вторгнення хакерів в їх комп'ютери, а 94% мали неприємності від вірусів. Достатньо поширеним щодо комп'ютерних злочинців є термін «хакер». Хакер – це особа, яка зламує комп'ютерні системи та мережі з метою фінансової наживи чи інших злодіянь, або заради завоювання авторитету в хакерських колах. Спочатку цей термін не був суто кримінально-правовим. Вперше в американському журналі «Тар», цей термін став використовуватися для визначення особи, яка невпорядкованими наборами телефонних иомерів, підключаються до чужих розмов. Сьогодні ж поняття «хакерство» в світі набуло кримі-

нально-правового змісту. Хакерами звуть осіб, які, володіючи зазначеними вище вміннями та досвідом, спрямовують свою діяльність на шкоду іншим особам, вчинюючи злочини в комп'ютерних системах. Тому, використовуючи термін «хакерство» щодо певного кола комп'ютерних злочинів, перш за все розуміють несанкціонований доступ до комп'ютерних систем. Суть несанкціонованого доступу до комп'ютерної системи полягає в протиправному доступі до комп'ютерної інформації, що належить іншому власнику (користувачу). Для того, щоб отримати доступ до захищеної комп'ютерної системи, власник (користувач) повинен ввести в неї при посередництві електронно-обчислювальної машини пароль доступу. Хакери використовують безліч різних засобів для того, щоб розпізнати секретні паролі або взагалі обійти парольно-кодовий захист системи і «увійти» в комп'ютерну систему. Опинившись «в середині комп'ютерної системи», хакер може прочитати, змінити, ліквідувати або скопіювати дані, що зберігаються в носіях комп'ютерної інформації. Особливу увагу фахівців сьогодні привертає і злочинне розповсюдження комп'ютерного вірусу та інших шкідливих програмних засобів, здатних проникати в автоматизовані системи та руйнувати комп'ютерну інформацію шляхом впливу на програмному рівні.

В моєму випадку комп'ютерна злочинність або кіберзлочинність, може бути визначена як будь-які протиправні діяння, при яких електронно-обчислювальні машини, системи електронно-обчислювальних машин або комп'ютерні мережі, комп'ютерна інформація або її носії виступають предметом або знаряддям злочинного діяння. При цьому, поняття комп'ютерної злочинності (кіберзлочинності) є предметом дослідження кримінології. Поняття «злочини в сфері використання комп'ютерних систем» належать до предмету дослідження кримінального права.

Важливою є проблема відсутності єдиного понятійного апарату та норм, щодо кваліфікації комп'ютерних злочинів, зокрема, пов'язаних з незаконним вручанням в роботу комп'ютерних систем. Так, в Резюме Десятого Конгресу Організації Об'єднаних Націй по попередженню злочинності і поводженню з правопорушниками, який відбувся в Відні 10-17 квітня 2000 року, вказано: «Для ефективного попередження кіберзлочинності і боротьби з нею необхідний узгоджений міжнародний підхід на різних рівнях. На внутрішньому рівні для розслідування кіберзлочинів потрібен належний персонал, спеціальний досвід, знання та процедури. На міжнародному рівні для розслідування кіберзлочинів необхідні оперативні дії, що спираються на координацію зусиль національних правоохоронних органів і прийняття відповідних юридичних підстав». Крім того, однією з проблем викриття комп'ютерних злочинів є недосконалість внутрішнього законодавства окремих держав. Так, щодо інформаційного законодавства України представники захисту вказують, що має місце розбіжність щодо розуміння структури і складу системи законодавства у сфері інформаційних відносин та підходів до їх формування, а також що нові правові акти у сфері суспільних інформаційних відносин нерідко не узгоджені концептуально з раніше прийнятими, що призводить до правового хаосу. Така необхідність в окремих державах закріплена в нормативних актах. Так, в Доктрині інформаційної безпеки Російської Федерації прямо вказується, що суперечливість і нерозвиненість правового регулювання суспільних відносин в інформаційній сфері призводять до серйозних негативних наслідків. Як вказують фахівці, ефективне рішення проблеми комп'ютерних злочинів вимагає узгоджених міжнародних дій і співробітництва. Однак, це можливо лише в тому випадку, якщо існує загальне розуміння проблеми як такої і необхідності розгляду відповідних рішень.

З метою уніфікації диспозицій статей кримінального законодавства країни-учасниць Ради Європи, як вказують, Комітет з юридичних питань Ради Європи розробив спеціальні Рекомендації № R (89) 9, які містять:

1) мінімальний перелік комп'ютерних правопорушень, який має бути включений у внутрішнє законодавство країн-учасниць Ради Європи;

2) вибірковий перелік комп'ютерних правопорушень, щодо включення яких у власне законодавство кожна країна вільна у прийнятті рішення.

Таким чином до мінімального переліку належать: комп'ютерне шахрайство, комп'ютерна підробка, пошкодження комп'ютерної інформації або комп'ютерних програм, комп'ютерний саботаж, несанкціонований доступ до комп'ютерної системи або мережі, несанкціоноване перехоплення інформації, несанкціоноване копіювання захищених комп'ютерних програм, незаконне копіювання топології мікросхем. До вибіркового переліку належать несанкціонована заміна інформації або комп'ютерних програм, комп'ютерне шпигунство, протиправне використання комп'ютера, несанкціоноване використання захищених комп'ютерних програм.

Загальносвітові вимоги боротьби з комп'ютерною злочинністю передбачають необхідність розробки в кожній державі власних норм щодо захисту від посягань на дані, що зберігаються в автоматизованих системах. Даний інститут кримінального права в Україні ще недостатньо розроблений. Однак, разом з поширенням Internet і зростанням загрози від комп'ютерної злочинності суспільним інтересам України, законодавець має визначити коло комп'ютерних злочинів, чітко розробивши норми, за якими буде можливо притягнути до відповідальності винних у їх вчиненні.

Високий рівень розкриття комп'ютерних злочинів, зокрема, в США, Франції, Німеччині, обумовлений ефективним законодавчим регулюванням відповідаль-ності за протиправні посягання на роботу комп'ютерних систем та комп'ютер-ну інформацію. Кримінальні кодекси республік колишнього СРСР не передбачали кримінальної відповідальності за втручання в роботу комп'ютерних систем. При цьому, перший злочин, вчинений з використанням комп'ютера, на території СРСР було офіційно зареєстровано в 1979 році в м. Вільнюс. Сучасні держави-учасниці Співдружності Незалежних Держав (далі – країни СНД), розуміючи необхідність захисту суспільства від будь-яких посягань, що вчинюються при посередництві комп'ютерних систем, вводять в своє внутрішнє законодавство норми, що передбачають захист інформаційних ресурсів та комп'ютерних систем та кримінальну відповідальність за комп'ютерні злочини. Так, основними цілями захисту інформації, у відповідності з законодавством Російської Федерації, названі: запобігання витіканню, розкраданню, перекручуванню, підробці інформації; запобігання небезпеці для особистості та держави; запобігання несанкціонованим діям по знищенню, перекручуванню, блокуванню інформації. Кримінальним кодексом Російської Федерації передбачено кримінальну відповідальність за такі злочини в сфері комп'ютерної інформації. Аналогічний підхід до законодавчого викладення норм, що визнають кримінально-караними діяння по незаконному втручанню в роботу комп'ютерних систем, з виділенням таких норм в окремі розділи особливих частин кримінальних кодексів, крім Російської Федерації зустрічаються в кримінальних кодексах таких країн: Азербайджанська Республіка, Грузія, Киргизька Республіка, Туркменістан. Формулювання диспозицій статей кримінальних кодексів вказаних держав тотожно нормам КК РФ, на мою думку, є наслідком необміркованої «трансплантації» норм, що передбачають відповідальність за злочини в сфері комп'ютерної інформації. В деяких країнах СНД злочини, що посягають на комп'ютерні системи або інформаційну безпеку, не виділені в самостійні розділи особливих частин кримінальних кодексів, а містяться в інших розділах.

Під час дослідження, також було звернено увагу на кримінальні кодекси Республіки Білорусь, Естонської Республіки та Республіки Таджикистан які, на відміну від інших кодексів країн, що розташовані на території колишнього СРСР, передбачають

кримінальну відповідальність за значно більший перелік суспільно-небезпечних діянь в сфері безпеки застосування комп'ютерних систем. Так, в Кримінальному кодексі Республіки Білорусь виділено в окремій главі 31 «Злочини проти інформаційної безпеки» шість статей, які передбача-ють кримінальну відповідальність за безпосереднє втручання в роботу комп'ютерних систем. Випливаючи з попередніх даних в законодавчому визначенні основних видів злочинів, що посягають на безпеку застосування комп'ютерних систем в країнах – колишніх республіках СРСР, викликало необхідність прийняття єдиних заходів, які б надавали можливість узгодження таких формулювань, як з метою їх вдосконалення, так і з метою застосування їх до осіб, що вчинюють комп'ютерні злочини на території СНД.

Висновки. В процесі дослідження норм міжнародного права, законодавства України та зарубіжних країн, які регламентують відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, їх систем та комп'ютерних мереж, мною було зроблено наступні висновки:

– особливої уваги вимагає аналіз комп'ютерних злочинів, які можуть вчинюватись як окремо, так і в сукупності з іншими злочинами, виступаючи способом вчинення останніх;

– комп'ютерна злочинність може бути визначена, як будь-які протиправні діяння, при яких електронно-обчислювальні машини, системи електронно-обчислювальних машин, або комп'ютерні мережі, комп'ютерна інформація або її носії виступають предметом або знаряддям злочинного діяння;

– комп'ютерна злочинність являє собою певний вид транснаціональної злочинності, а злочини, які посягають на безпеку використання комп'ютерних систем, належать до транснаціональних.

Очевидна наявність вказаних причин свідчить про необхідність детальної комплексної кримінально-правової характеристики незаконного втручання в роботу електронно-обчислювальних машин, їх систем та комп'ютерних мереж.

Список літератури: 1. Сташис В.В., Тація В.Я. Кримінальний кодекс України: Наук.-практ. коментар / За заг. ред. – К., 2006. – С. 969. 2. Голубєв В.О. та ін. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. / За заг. ред. професора Калюжного Р.А. – Запоріжжя: Просвіта, 2001. – 257 с. 3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР.